ITRI 615

Whitman & Mattord Chapter 9

Physical Access Controls

- In facilities management, a secure facility is a physical location that has in place controls to minimize the risk of attacks from physical threats (see Amy Windahl was back early from lunch p. 467 and offline guard duty, p. 472).

- Some physical access controls that can aid with securing a facility include:

1. Walls, fencing and gates.

2. Guards.

3. Dogs.

4. ID cards and badges.

Physical Access Controls *cont.*

5. Locks and keys.
6. Mantraps. See figure 9.3, p. 476.
7. Electronic monitoring.
8. Alarms and alarm systems.
9. Computer rooms and wiring closets.
10. Interior walls and doors.

Fire security and safety

- The most serious threat to people in an organization is fire.
- It accounts for more property damage, personal injury, and death than any other threat to physical security.
- Fire suppression systems are devices that are installed and maintained to detect and respond to a fire, potential fire, or combustion danger situation.
- The flame point, or temperature of ignition, depends on the material and can be as low as a few hundred degrees.

Fire security and safety *cont.*

- Fire detection can be either manual or automatic. Manual typically through human responses, and automatic through devices.

- There are three types of automatic fire detection systems.

1. Thermal detection systems. Contains a heat sensor that reacts either to a high temperature or to a rapid rise in temperature.

2. Smoke detection. Based on photoelectric sensors, ionization sensors, or air-aspirating detectors.

3. Flame detectors. Detects the infrared or ultraviolet light produced by an open flame.

Fire suppression

- Can consist of portable, manual or automatic apparatus.

- Portable extinguishers are used for smaller fires and where fixed apparatus is impractical.

- Portable extinguishers are rated by the type of fire they can combat, as follows:

1. Class A. Fires that involve ordinary combustible fuels.
2. Class B. Fires fueled by combustible liquids or gases.
3. Class C. Fires with energized electrical appliances or equipment.
4. Class D. Fires fueled by combustible metals.

Fire suppression *cont.*

- Manual and automatic systems are those designed to apply suppressive agents. They are usually either sprinkler or gaseous systems.

- Sprinkler are divided into three implementations, namely:

1. Wet-pipe. Contains pressurized water in all pipes.

2. Dry-pipe. Contains pressurized air, which is released before the water. Reduces the risk of accidental leakage.

3. Pre-action. Two phase process whereby stage one involves filling the pipes with water, and stage two then involves manual activation of individual sprinklers.

Fire suppression *cont.*

- Gaseous emission systems are often used to protect chemical and electrical processing areas, as well as facilities that house computing systems (see figure 9.5 p. 519).
- Can be either self-pressurizing or pressurized with an additional agent.
- Only two major types, using either carbon dioxide or Halon.
- Unlike carbon dioxide, Halon does not extinguish life forms that are dependent on oxygen as well. It is however an ozone-depleting substance, and is no longer used in suppression systems. Many alternatives are available.

Failure of supporting utilities

- Failure of supporting utilities can have a significant impact on the safe operation of a facility. Each of these utilities must be properly managed in order to prevent damage to information and information systems. These utilities include:

1. Heating, ventilation, and air conditioning.

2. Temperature and filtration.

3. Humidity and static electricity.

4. Ventilation shafts.

Failure of supporting utilities *cont.*

5. Power management and conditioning.
6. Grounding and amperage.
7. Uninterruptible power supply.
8. Emergency shutoff.
9. Water problems.
10. Structural collapse.
11. Maintenance of facility systems.

Interception of data

- Direct observation. Requires that an individual be close enough to the information to breach confidentiality. Major risk is when information is removed from a secure facility.

- Interception of data transmissions. When attackers can access the media transmitting the data, they don't have to be close to the source. Includes tapping into a LAN, eavesdropping over a wireless LAN, etc.

- Electromagnetic interception. Eavesdropping on the electromagnetic signals emitted when electricity moves through cables. Has been hotly debated whether this is actually possible, despite the fact that the US government and military are investing a good deal of money in securing their systems from EM interception.

Questions

- Any questions?